



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,323	07/01/2004	David S. Bonalle	70655.2100	4322
20322	7590	03/09/2006	EXAMINER	
SNELL & WILMER ONE ARIZONA CENTER 400 EAST VAN BUREN PHOENIX, AZ 850040001			WALSH, DANIEL I	
			ART UNIT	PAPER NUMBER
			2876	

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/710,323

Applicant(s)

BONALLE ET AL.

Examiner

Daniel I. Walsh

Art Unit

2876

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-46 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 7-04, 8-04.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

1. Receipt is acknowledged of the IDS received on 1 July 2004 and 5 August 2004.

Claim Objections

2. Claims 1 and 16 are objected to because of the following informalities:

Re claim 1: Replace “a reader configured” with -- said reader configured --.

Re claim 16: Replace “DNA scan sample is primarily” with – a first DNA scan sample is primarily – and “DNA scan sample is secondarily” with – a second DNA scan sample is secondarily --.

Appropriate correction is required.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-46 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-46 of copending Application No. 10/708,830. Although the conflicting claims are not identical, they are not patentably distinct from each other because the '830 Patent Application recites a transponder reader system, while the current Patent Application recites a smartcard system. However, the Examiner notes that smart cards and transponders can be used interchangeably, and are obvious expedients based on design or system constraints. The interchangeability/obviousness of such devices is taught by Black (see below), which uses smartcards and transponders interchangeably.

i) For example, in claim 1 of the current Patent Application the Applicants claim: "A smartcard transaction system....DNA scan sensor...facilitate a transaction." (see claim 1), whereas in the '830 Patent Application the Applicants claim: "A transponder-reader transaction system....DNA scan sensor...facilitate a payment transaction." (see claim 1)

ii) For example, in claim 22 of the current Patent Application the Applicants claim: "A method for facilitating...smartcard...DNA scan...authorization of a transaction." (see claim 22), whereas in the '830 Patent Application the Applicants claim: "A method for facilitating...transponder-reader...DNA scan...authorization of a payment transaction." (see claim 22).

iii) For Example, in claim 34 of the current Patent Application the Applicants claim: "A method for facilitating...smartcard...DNA scan...proffered DNA sample." (see claim 34),

whereas in the '830 Patent Application the Applicants claim: "A method for facilitating...transponder-reader...DNA scan...proffered DNA scan sample." (see claim 34).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-15, 17, and 19-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black (US 6,925,565), in view of Simon (US 2003/0086591).

Re claim 1, Black teaches a smartcard configured to communicate with a reader, a reader configured to communicate with the system, a biometric sensor to detect a fingerprint sample, the sensor configured to communicate with the system (FIG. 1A). Though silent to a verification device to verify the sample, the Examiner notes that a transaction is authorized upon verification of the sample. Therefore, at the time the invention was made, it would have been obvious to have a verification device in order to verify the sample as part of the authentication (security).

Black is silent to the biometric/scan sample being a DNA scan sample.

The Examiner notes that DNA is well known and conventional in the art to be used for authentication purposes. It would have been an obvious expedient to use DNA as an alternative means to identify a person, with enhanced security. Additionally, the Examiner directs the Applicant to the relevant art cited at the end of the action, which includes references that teach that fingerprint biometrics can be replaced with other biometrics, including voice prints, thus obviating such alternative biometrics. Nonetheless, Simon teaches that DNA sampling to verify a user (paragraph [0013] and paragraph [0018]), where the sensor can be on the card, a separate unit, etc.

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Simon.

One would have been motivated to do this in order to have different forms of biometric identification, well known and conventional in the art, to verify a user securely.

Re claim 2, the Examiner notes that the sensor communicates with the system via at least one of a smartcard, reader, and network (FIG. 1A of Black).

Re claim 3, it is understood that the biometric sensor is configured to facilitate a finite number of scans (one for example) in order to receive a sample (namely one).

Re claim 4, FIG. 5A+ (of Black) shows that the fingerprint biometric sensor logs/stores at least one of a detected fingerprint sample, processed sample, and stored sample. Accordingly, it would have been obvious to log the DNA sample for such record keeping purposes.

Re claims 5-6, Black teaches (col 6, lines 56+) that the customer record can be stored locally or remotely. The Examiner notes that though Black is silent to a datapacket stored on a database, Black teaches that the customer record can include biometric information, user information, etc. (FIG. 5A+ for example). Therefore, the Examiner notes that it would be within the skill in the art for such a collection of data can be interpreted as a data packet (and to include the DNA data as discussed above). It would have been obvious to store such information on a database, in order to have a well-known and conventional means of storing data for quick retrieval and organization. It has been discussed above that the data can be stored remotely or locally. Accordingly, it would have been obvious to one of ordinary skill in the art to store it on the smartcard or a remote device based on security needs.

Re claim 7, it has been discussed above that samples are received and stored for providing security/authentication. It would have been obvious for the samples to be received by an authorized receiver in order to ensure security and reliability.

Re claim 8, though Simon teaches a DNA scan sensor device, Simon is silent to it having at least an infrared or chemical sensor. The Examiner notes that such a sensor is well known and conventional for DNA sensors, and therefore is an obvious expedient to detect a proffered DNA sample.

Re claim 9, it is well known and conventional in the art for DNA to be verified against nucleotides, code sequences, regulatory regions, initiation codons, stop codons, exon borders, intron borders, etc. as means to verify DNA, as such means provide a way to identify samples (properties). Simon teaches matching DNA to a sequence (paragraph [0018]), interpreted as a code sequence of the DNA.

Re claim 10, the Examiner notes that Black/Simon are silent to detecting and verifying false DNA and thermal patterns. However, the Examiner notes that if the DNA sample provided to the sensor does not match a stored sample or is not an adequate sample, an error or mismatch would result. Accordingly, such a function can be interpreted as detecting/verifying false DNA (DNA that does not match).

Re claim 11, the Examiner notes that such security procedures are well known and conventional in the art for ensuring the authenticity of samples (Applicants own specification). As discussed above by Simon and the abstract of Black, a proffered DNA/biometric sample is compared to a stored sample (a record) to verify the user/DNA/biometric.

Re claim 12, it has been discussed above that a comparison is performed. The Examiner notes that it would have been obvious to one of ordinary skill in the art to use a local CPU/third party security vendor device to electronically perform the comparison, in order to have an electronic (automated) means to quickly and reliably perform the comparison, as is conventional in the art. Black teaches (above) that the comparison is performed electronically. As such, the use of such a local CPU/third party security vendor to perform the comparison is an obvious expedient to accurately/electronically perform the comparison process.

Re claim 13, the Examiner notes that as a sample is stored, it's interpreted as registered.

Re claim 14, Black teaches that a customer's account is linked to the sample data, and can be used for payment and is linked to a credit or debit account (abstract, col 6, lines 46+).

Re claim 15, the Examiner notes that it is obvious that the system of Black would be used by a plurality of customers. As such, it would have been obvious that different people have different samples (unique), which would be associated with their different accounts.

Re claim 17, as Black teaches an account is only accessed after a sample is verified, it is interpreted as beginning authentication after verification of the sample.

Re claim 19, though Black is silent to the sensor providing notification upon detection of a sample, the Examiner notes that it is well within the skill in the art to provide notification that a sample has been detected, in order to provide indication to the user, that the sample was received and they don't have to keep offering a sample (suitable indications that electronic operations have been completed include audible information, textual information, etc., as is conventional in electronic transactions). As Black indicates when a sample has been authorized (transaction allowed) it would have been obvious to indicate when the sample is read/detected as a means to provide guiding information to the user. Additionally, the Examiner notes that the mere authorization of a transaction can be broadly interpreted as providing notification upon detection of a sample because authorization cannot occur unless the sample was detected.

Re claim 20, it has been discussed above that the device facilitates a financial transaction.

Re claims 21 and 33, though silent to secondary security procedures, the Examiner notes that such procedures such as PINs, codes, passwords, additional identifiers etc. are well known and conventional in the art. One would have been motivated to use such procedures for increased security. Additionally, Simon teaches additional/secondary sensors 208/210.

Re claim 22, Black/Simon teach a method for facilitating biometric security in a smartcard/reader system comprising providing a DNA scan to a DNA scan sensor communicating with the system to initiate verification of a biometric for facilitating authorization of a transaction, as discussed above.

Re claim 23, the Examiner has interpreted the storing of the sample with the system as an authorized sample receiver.

Re claim 24, registering includes proffering a sample (abstract, FIG. 5A of Black).

Re claim 25, the limitations have been discussed above re claim 8.

Re claim 26, Black teaches that a sample is stored and that proffered samples are compared and verified to complete a transaction (abstract).

Re claim 27, Black teaches the step of proffering a biometric to a sensor communicating with the system to initiate verification, as discussed above. As discussed above, Black teaches that the information can be stored on the smartcard itself or remotely, depending on the desired security. Though silent to a database, a database is an obvious expedient as discussed above. Accordingly, it would have been obvious to process database information contained in at least one of the smartcard, reader, sensor, server, and reader system as a means to authenticate/verify a user. The storage location of verification information can be varied based on security needs, as discussed above.

Re claim 28, Black teaches comparing the proffered sample with stored sample (abstract).

Re claims 29, the limitations have been discussed above, re claim 12.

Re claim 30, the limitations have been discussed above re claim 9.

Re claim 31, the limitations have been discussed above re claim 10.

Re claim 32, the Examiner notes that as the system is used with more than one user (therefore more than one sample) it would have been obvious to detect/process/store a second sample (of additional users).

Re claim 34, Black/Simon teaches a method of facilitating biometric security in a smartcard reader transaction system comprising detecting a proffered DNA scan at a sensor communicating with the system to obtain a proffered sample, verifying the sample, and authorizing a transaction to proceed upon verification of the sample (as discussed above.)

Re claim 35, Black teaches that the sample is detected at a sensor configured to communicate with the system via one of a smartcard/reader/network (FIG. 1A-1C).

Re claim 36, the limitations have been discussed above re claim 8.

Re claim 37, the limitations have been discussed above.

Re claim 38, receiving a finite number of scans has been discussed above (namely one sample).

Re claim 39, the storing/logging of samples is an obvious expedient for record keeping purposes, and has been discussed above. Additionally, the Examiner notes that samples are stored/logged at least temporarily (in a buffer) in typical comparison processes.

Re claim 40, the limitations have been discussed above re claim 10.

Re claim 41, as discussed above, it would have been obvious to one of ordinary skill in the art to detect/process/store a second sample, when the system is used by different people with different accounts and samples.

Re claim 42, the comparison of a proffered sample to a stored/registered sample has been discussed above.

Re claim 43, the limitations have been discussed above re claim 9.

Re claim 44, the Examiner notes that the proffered biometric is indeed compared with a sample of at least one of a criminal, terrorist, and card member, as the sample is compared to a current card members sample, to authorize the transaction.

Re claim 45, verifying the sample using information contained on one of a local database/remote database/third party controlled database would have been an obvious expedient in instances where the data is stored remote from the smartcard (as discussed above, based on security concerns). The biometric would be verified by using information contained in a database, as a preferred means to organize data for efficient and easy storage and retrieval (remote or local).

Re claim 46, the verification of a sample using a protocol/sequence controller (interpreted as a processor) has been discussed above.

5. Claims 15, 32, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Simon, as discussed above, in view of Martizen et al. (US 2002/0191816).

The teachings of Black/Simon have been discussed above.

Black/Simon is silent to different samples (of the same person) associated with different one of personal information, credit card information, etc. as claimed.

Martizen et al. teaches different registered biometric samples are associated with different personal information (different fingers with different accounts) (FIG. 6A).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Simon with those of Martizen et al.

One would have been motivated do to this to permit multiple accounts to be securely accessed with different samples, for user convenience and security. Though Martizen et al. teaches fingerprint samples, it has been discussed above that a DNA sample is an obvious expedient for uniquely identifying an individual, and is an alternative means for doing so. Accordingly, different types of DNA (hair, spit, blood, etc., which are well known and conventional in the art)samples would be an obvious expedient for identification, based on the teachings of Martizen et al.

6. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Simon/Martizen et al., as discussed above, in view of Moebs et al (US 2005/0065872).

The teachings of Black/Simon/Martizen et al. have been discussed above.

Black/Simon/Martizen et al. are silent to primary and secondary associating.

The Examiner notes that such associating is well known in the art (line of credit, for example). Specifically, Moebs et al. teaches that a customer can avoid overdraft by preauthorizing the financial institution to tie the customers' checking account to one or more of the customers other accounts (paragraph [0017]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Simon/Martizen with those of Moebs et al.

One would have been motivated to do this in order to provide for overdraft protection, for example.

7. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Simon, as discussed above, in view of Goodman (US 2002/0043566).

The teachings of Black/Simon have been discussed above.

Black teaches that the transaction is blocked when the biometrics do not match, as is conventional in the art, but Black is silent to deactivation upon rejection of the sample.

The Examiner notes that it is well known and conventional in the art for card to be disabled, as a security measure, if a predetermined amount of failed attempts are detected, for example. Specifically, Goodman et al. teaches deactivation of a card if a predetermined amount of incorrect PIN attempts are detected (paragraph [0029]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Simon with those of Goodman et al.

One would have been motivated to do this in order to increase system security.

Though Goodman et al. is silent to a biometric input, the Examiner notes that Goodman et al. is relied upon for teaching disabling of access when a matching input is not received. It would have been obvious to disable the smartcard when biometrics don't match (biometrics replacing PIN input, as a more secure alternative).

8. Claims 4, 21, 33, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Simon, as discussed above, in view of Black (US 2005/0122209).

The teachings of Black/Simon have been discussed above.

Re claims 21 and 33, Black/Simon is silent to secondary security procedures. Re claims 4 and 40, Black is silent to logging each proffered fingerprint sample.

Black '209 teaches such procedures through signature verification (abstract). Black '209 teaches storing of digital and electronic signature for record keeping purposes (paragraph [0125]). Simon teaches secondary sensors as discussed above.

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Simon with those of Black '209.

One would have been motivated to do this for increased security and record keeping purposes.

Additional Remarks

9. As an example, Janiak et al. (US 2002/0097142) teaches user indication. User indication is well known in the art to keep the user informed during a process. Typical user indication is readily seen at checkouts/point of sale devices, for example.

McCall et al. (US 2003/0132297) stores/logs signatures.

Haala et al. (US 2005/0102524) teaches recording details if authentication fails.

Segal et al. (US 2002/0066784) teaches bundling a signature with transaction database to effect proof of a transaction.

Hoshino et al. (US 6,636,620) teaches a biometric system.

Kita (US 6,703,918) teaches a transponder biometric system (FIG. 15+).

Rowe (US 2004/0050930) teaches a DNA smartcard with onboard authentication.

10. Additionally, the Examiner notes that it is unclear as to whether the claims (15, 32, and 40) are based upon different DNA samples of different people or of one user. Appropriate clarification is requested.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Haala (US 2005/0102524), Janiak et al. (US 2002/0097142), and McCall et al. (US 2003/0132297), Rowe (US 2004/0050930), Kita (US 6,703,918), and Hoshino et al. (US 6,636,620).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel I. Walsh whose telephone number is (571) 272-2409. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

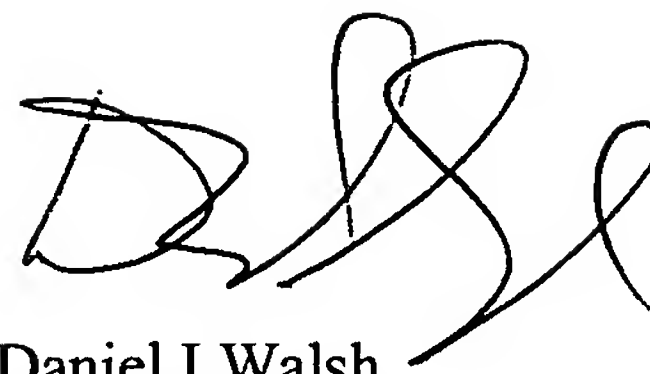
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 10/710,323

Art Unit: 2876

Page 16

D. Walsh

A handwritten signature in black ink, appearing to read 'D. Walsh', with a stylized, cursive flourish extending from the end.

Daniel I Walsh

Examiner

Art Unit 2876

2-27-06